Standar Nasional Indonesia

SNI ISO/IEC 27001:2013

Teknologi informasi – Teknik keamanan – Sistem manajemen keamanan informasi – Persyaratan

Information technology – Security techniques – Information security management systems – Requirements

(ISO/IEC 27001:2013, IDT)

ICS 35.040

Badan Standardisasi Nasional

Daftar isi

Prakata

Standar Nasional Indonesia (SNI) ISO/IEC 27001:2013 dengan judul *Teknologi informasi – Teknik keamanan – Sistem manajemen keamanan informasi – Persyaratan,* merupakan adopsi identik dari ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements,* dengan metode terjemahan dua bahasa, sebagai pengganti dari publikasi standar terbitan tahun 2013 yang menggunakan metode republikasi-*reprint*. Standar ini merupakan revisi dari SNI ISO/IEC 27001:2009*, Teknologi informasi – Teknik keamanan – Sistem manajemen keamanan informasi – Persyaratan.*

Standar ini disusun oleh Komite Teknis 35-01, *Teknologi Informasi*. Standar ini telah dibahas dan disetujui dalam rapat konsensus nasional di Bogor pada tanggal 28 November 2013. Konsensus ini dihadiri oleh para pemangku kepentingan (*stakeholder*) terkait, yaitu perwakilan dari produsen, konsumen, pakar dan pemerintah.

Dalam standar ini istilah "*this International Standard*" diganti menjadi "*this Standard*", dan diterjemahkan menjadi "Standar ini".

Terdapat beberapa standar ISO/IEC yang dijadikan sebagai acuan dalam standar ini telah diadopsi menjadi Standar Nasional Indonesia (SNI), yaitu:

1) ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management,* telah diadopsi secara identik menjadi SNI ISO/IEC 27002:2013, *Teknologi Informasi – Teknik keamanan – Panduan praktik manajemen keamanan informasi.*

2) ISO/IEC 27003:2010, *Information technology – Security techniques – Information security management system implementation guidance,* telah diadopsi secara identik menjadi SNI ISO/IEC 27003:2013, *Teknologi Informasi – Teknik keamanan – Panduan implementasi sistem manajemen keamanan informasi.*

3) ISO/IEC 27004:2009, *Information technology – Security techniques – Information security management – Measurement,* telah diadopsi secara identik menjadi SNI ISO/IEC 27004:2013, *Teknologi Informasi – Teknik keamanan – Manajemen keamanan informasi – Pengukuran.*

4) ISO/IEC 27005:2011, *Information technology – Security techniques – Information security risk management,* telah diadopsi secara identik menjadi SNI ISO/IEC 27005:2013, *Teknologi Informasi – Teknik keamanan – Manajemen risiko keamanan informasi.*

Apabila pengguna menemukan keraguan dalam standar ini maka disarankan untuk melihat standar aslinya yaitu ISO/IEC 27001:2013 (E) dan/atau dokumen terkait lain yang menyertainya.

Pendahuluan

0.1 Umum

Standar ini dibuat untuk menyediakan persyaratan untuk penetapan, penerapan, pemeliharaan, dan perbaikan berkelanjutan terhadap Sistem Manajemen Keamanan Informasi (SMKI). Adopsi SMKI merupakan keputusan strategis organisasi. Penetapan dan penerapan SMKI dipengaruhi oleh kebutuhan dan tujuan organisasi, persyaratan keamanan, proses organisasional yang digunakan, dan ukuran dan struktur organisasi. Semua faktor yang mempengaruhi ini diharapkan berubah seiring waktu.

SMKI melindungi kerahasiaan *(confidentiality),* keutuhan *(integrity),* dan ketersediaan *(availability)* informasi dengan menerapkan proses manajemen risiko dan memberikan kepercayaan kepada pihak yang berkepentingan bahwa risiko dikelola secara memadai.

Penting difahami bahwa SMKI merupakan bagian dari dan teritegrasi dengan proses organisasi dan struktur manajemen keseluruhan, dan bahwa keamanan informasi dipertimbangkan dalam desain proses, sistem informasi, dan pengendalian. Penerapan SMKI diharapkan akan ditingkatkan sesuai kebutuhan organisasi.

Standar ini dapat digunakan oleh pihak internal dan eksternal untuk menilai kemampuan organisasi dalam memenuhi persyaratan keamanan informasi organisasi itu sendiri.

Urutan persyaratan yang disajikan dalam Standar ini tidak mencerminkan pentingnya persyaratan itu, atau tidak menyiratkan urutan persyaratan yang harus dilaksanakan. Daftar item disebutkan hanya untuk tujuan referensi.

SNI ISO/IEC 27000 menjelaskan gambaran dan kosakata SMKI, yang mengacu keluarga standar SMKI (termasuk ISO/IEC 27003[2], ISO/IEC 27004[3] and ISO/IEC 27005[4]), dengan istilah dan definisi yang terkait.

0.2 Kompatibilitas dengan standar sistem manajemen lainnya

Standar ini menerapkan struktur tingkat-tinggi, judul sub-klausul identik, teks identik, istilah umum, dan definisi inti yang didefinisikan dalam Lampiran SL ISO Directive/IEC, Bagian 1, Tambahan ISO Konsolidasi, sehingga menjaga kompatibilitas dengan standar sistem manajemen lainnya yang telah mengadopsi Annex SL.

Pendekatan umum yang didefinisikan dalam Lampiran SL ini akan berguna bagi organisasi yang memilih untuk mengoperasikan sistem manajemen tunggal yang memenuhi persyaratan dari dua atau lebih standar sistem manajemen.

Teknologi informasi – Teknik keamanan – Sistem manajemen keamanan informasi – Persyaratan

1 Ruang lingkup

Standar ini menentukan persyaratan untuk menetapkan, menerapkan, memelihara dan secara berkelanjutan memperbaiki Sistem Manajemen Keamanan Informasi (SMKI) dalam konteks organisasi. Standar ini juga mencakup persyaratan untuk penilaian dan penanganan risiko keamanan informasi disesuaikan dengan kebutuhan organisasi. Persyaratan yang ditetapkan dalam Standar ini bersifat umum dan dimaksudkan untuk dapat diterapkan pada semua organisasi, terlepas dari jenis, ukuran atau sifat organisasi. Setiap persyaratan yang ditetapkan dalam Klausul 4 hingga 10 tidak dapat dikecualikan bila organisasi menyatakan kesesuaian terhadap Standar ini.

2 Acuan normatif

Dokumen acuan berikut, seluruh atau sebagian, secara normatif dirujuk dalam dokumen ini dan sangat diperlukan dalam penerapannya. Untuk acuan bertanggal, hanya berlaku edisi yang disebutkan. Untuk acuan tidak bertanggal, berlaku edisi terakhir dari dokumen acuan (termasuk setiap amandemen).

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Istilah dan definisi

Untuk dokumen ini, berlaku istilah dan definisi yang diberikan dalam ISO/IEC 27000.

4 Konteks organisasi

4.1 Memahami organisasi dan konteksnya

Organisasi harus menetapkan masalah eksternal dan internal yang relevan dengan tujuan dan yang mempengaruhi kemampuannya untuk mencapai hasil yang diharapkan dari SMKI organisasi.

CATATAN Penentuan masalah ini mengacu penetapan konteks eksternal dan internal dari organisasi yang dipertimbangkan dalam Klausul 5.3 dari ISO 31000:2009[5].

4.2 Memahami kebutuhan dan harapan dari pihak yang bekepentingan

Organisasi harus menentukan:

a) pihak yang berkepentingan yang relevan dengan SMKI; dan

b) persyaratan pihak yang berkepentingan ini yang terkait dengan keamanan informasi.

CATATAN Persyaratan pihak yang berkepentingan dapat mencakup persyaratan hukum dan peraturan perundang undangan, serta kewajiban kontraktual.

4.3 Penentuan ruang lingkup SMKI

Organisasi harus menentukan batasan dan penerapan SMKI untuk menetapkan ruang lingkup SMKI.

Ketika menentukan ruang lingkup ini, organisasi harus mempertimbangkan:

a) masalah eksternal dan internal seperti yang disebutkan pada 4.1;

b) persyaratan seperti yang disebutkan pada 4.2; dan

c) antarmuka dan ketergantungan antara kegiatan yang dilakukan oleh organisasi, dan kegiatan yang dilakukan oleh organisasi lain.

Ruang lingkup harus tersedia sebagai informasi yang terdokumentasi.

4.4 Sistem manajemen keamanan informasi

Organisasi harus menetapkan, menerapkan, memelihara dan memperbaiki secara berkelanjutan SMKI, sesuai dengan persyaratan Standar ini.

5 Kepemimpinan

5.1 Kepemimpinan dan komitmen

Manajemen puncak harus menunjukkan kepemimpinan dan komitmen terkait SMKI dengan cara:

a) memastikan kebijakan keamanan informasi dan sasaran keamanan informasi ditetapkan dan selaras dengan arah strategis organisasi;

b) memastikan persyaratan SMKI terintegrasi ke dalam proses organisasi;

c) memastikan tersedianya sumber daya yang dibutuhkan untuk SMKI;

d) mengomunikasikan pentingnya manajemen keamanan informasi yang efektif dan kesesuaian dengan persyaratan SMKI;

e) memastikan bahwa SMKI mencapai manfaat yang diharapkan;

f) memberikan arahan dan dukungan pada personel untuk berkontribusi dalam efektivitas SMKI;

g) mempromosikan perbaikan berkelanjutan; dan

h) mendukung peran manajemen yang relevan lainnya untuk menunjukkan kepemimpinannya ketika diterapkan pada wilayah tanggung jawabnya.

5.2 Kebijakan

Manajemen puncak harus menetapkan kebijakan keamanan informasi yang:

a) sesuai dengan tujuan organisasi;

b) mencakup sasaran keamanan informasi (lihat 6.2) atau menyediakan kerangka kerja untuk menetapkan sasaran keamanan informasi;

c) mencakup komitmen untuk memenuhi persyaratan yang berlaku terkait dengan keamanan informasi; dan

d) mencakup komitmen untuk perbaikan berkelanjutan terhadap SMKI.

Kebijakan keamanan informasi harus:

e) disediakan sebagai informasi yang terdokumentasi;

f) dikomunikasikan dalam organisasi; dan

g) disediakan untuk pihak yang berkepentingan, jika diperlukan.

5.3 Peran organisasi, tanggung jawab dan wewenang

Manajemen puncak harus memastikan bahwa tanggung jawab dan wewenang untuk peran-peran yang relevan dengan keamanan informasi ditetapkan dan dikomunikasikan.

Manajemen puncak harus menetapkan tanggung jawab dan wewenang untuk:

a) memastikan bahwa SMKI sesuai dengan persyaratan dari Standar ini;

b) melaporkan kinerja SMKI kepada manajemen puncak.

CATATAN Manajemen puncak juga dapat menetapkan tanggung jawab dan wewenang untuk melaporkan kinerja SMKI dalam organisasi.

6 Perencanaan

6.1 Tindakan untuk menangani risiko dan peluang

6.1.1 Umum

Ketika merencanakan SMKI, organisasi harus mempertimbangkan permasalahan yang dimaksud dalam 4.1 dan persyaratan yang dimaksud dalam 4.2 serta menentukan risiko dan peluang yang perlu ditangani untuk:

a) memastikan SMKI dapat mencapai manfaat yang diharapkan;

b) mencegah, atau mengurangi, efek yang tidak diinginkan;

c) mencapai perbaikan yang berkelanjutan.

Organisasi harus merencanakan:

d) tindakan untuk menangani risiko dan peluang; dan

e) bagaimana cara:

1) mengintegrasikan dan menerapkan tindakan ke dalam proses SMKI; dan

2) mengevaluasi efektivitas tindakan tersebut.

6.1.2 Penilaian risiko keamanan informasi

Organisasi harus menetapkan dan menerapkan proses penilaian risiko keamanan informasi, yakni:

a) menetapkan dan memelihara kriteria risiko keamanan informasi yang meliputi:

1) kriteria keberterimaan risiko; dan

2) kriteria untuk melakukan penilaian risiko keamanan informasi;

b) memastikan bahwa penilaian risiko keamanan informasi yang diulang akan memberikan hasil yang konsisten, valid dan sebanding;

c) mengidentifikasi risiko keamanan informasi:

1) menerapkan proses penilaian risiko keamanan informasi untuk mengidentifikasi risiko yang terkait dengan hilangnya kerahasiaan, integritas dan ketersediaan informasi dalam ruang lingkup SMKI; dan

2) mengidentifikasi pemilik risiko;

d) menganalisis risiko keamanan informasi:

1) menilai konsekuensi potensial yang akan terjadi jika risiko yang teridentifikasi pada 6.1.2 c) 1) terjadi;

2) menilai kemungkinan realistis terjadinya risiko yang teridentifikasi pada 6.1.2 c) 1); dan

3) menentukan tingkat risiko;

e) mengevaluasi risiko keamanan informasi:

1) membandingkan hasil analisis risiko dengan kriteria risiko yang ditetapkan pada 6.1.2 a); dan

2) memprioritaskan risiko yang dianalisis untuk penanganan risiko.

Organisasi harus menyimpan informasi yang terdokumentasi tentang proses penilaian risiko keamanan informasi.

6.1.3 Penanganan risiko keamanan informasi

Organisasi harus menetapkan dan menerapkan proses penanganan risiko keamanan informasi untuk:

a) memilih opsi penanganan risiko keamanan informasi yang tepat, dengan mempertimbangkan hasil penilaian risiko;

b) menentukan semua kendali yang diperlukan untuk menerapkan opsi penanganan risiko keamanan informasi yang dipilih;

CATATAN Organisasi dapat merancang kendali yang diperlukan, atau mengidentifikasi kendali dari berbagai sumber.

c) membandingkan kendali yang ditentukan pada 6.1.3 b) di atas dengan yang ada dalam Lampiran A dan memverifikasi bahwa tidak terlewatnya kendali yang diperlukan;

CATATAN 1 Lampiran A berisi daftar lengkap dari sasaran kendali dan kendali. Pengguna Standar ini diarahkan pada Lampiran A untuk memastikan bahwa tidak terlewatnya kendali yang diperlukan.

CATATAN 2 Sasaran kendali secara implisit termasuk dalam kendali yang dipilih. Sasaran kendali dan kendali yang tercantum dalam Lampiran A belum mencakup keseluruhan dan mungkin diperlukan tambahan sasaran kendali dan kendali.

d) menghasilkan *Statement of Applicability* yang berisi kendali yang diperlukan (lihat 6.1.3 b) dan c)) dan alasan pencantuman, apakah kendali itu diterapkan atau tidak, dan alasan pengecualian kendali dari Lampiran A;

e) merumuskan rencana penanganan risiko keamanan informasi, dan

f) mendapatkan persetujuan pemilik risiko terhadap rencana penanganan risiko keamanan informasi dan keberterimaan risiko keamanan informasi yang tersisa.

Organisasi harus menyimpan informasi yang terdokumentasi tentang proses penanganan risiko keamanan informasi.

CATATAN Proses penilaian dan penanganan risiko keamanan informasi dalam Standar ini sejalan dengan prinsip-prinsip dan pedoman umum yang tersedia dalam ISO 31000[5].

6.2 Sasaran keamanan informasi dan perencanaan untuk mencapainya

Organisasi harus menetapkan sasaran keamanan informasi pada fungsi dan tingkatan yang relevan.

Sasaran keamanan informasi harus:

a) konsisten dengan kebijakan keamanan informasi;

b) dapat diukur (jika dapat diterapkan);

c) mempertimbangkan persyaratan keamanan informasi yang berlaku, dan hasil dari penilaian risiko dan penanganan risiko;

d) dikomunikasikan; dan

e) diperbarui jika diperlukan.

Organisasi harus menyimpan informasi terdokumentasi mengenai sasaran keamanan informasi.

Ketika merencanakan bagaimana mencapai sasaran keamanan informasinya, organisasi harus menetapkan:

f) apa yang akan dilakukan;

g) sumber daya apa yang akan diperlukan;

h) siapa yang akan bertanggung jawab;

i) kapan akan selesai; dan

j) bagaimana hasilnya akan dievaluasi.

7 Dukungan

7.1 Sumber daya

Organisasi harus menentukan dan menyediakan sumber daya yang dibutuhkan untuk penetapan, penerapan, pemeliharaan dan perbaikan berkelanjutan terhadap SMKI.

7.2 Kompetensi

Organisasi harus:

a) menentukan kompetensi yang diperlukan untuk personel yang melakukan pekerjaan di bawah kendali organisasi yang mempengaruhi kinerja keamanan informasi organisasi;

b) memastikan bahwa personel ini kompeten berdasarkan pendidikan, pelatihan, atau pengalaman yang sesuai;

c) apabila memungkinkan, mengambil tindakan untuk memperoleh kompetensi yang diperlukan, dan mengevaluasi efektivitas tindakan yang diambil; dan

d) menyimpan informasi terdokumentasi yang sesuai sebagai alat bukti kompetensi.

CATATAN Tindakan yang bisa diterapkan dapat meliputi, misal: penyediaan pelatihan, bimbingan, atau penugasan kembali terhadap karyawan yang ada; atau merekrut atau mengontrak personel yang kompeten.

7.3 Kepedulian

Personel yang bekerja di bawah kendali organisasi harus peduli terhadap:

a) kebijakan keamanan informasi;

b) kontribusinya terhadap efektivitas SMKI, termasuk manfaat peningkatan kinerja keamanan informasi; dan

c) implikasi dari ketidaksesuaian dengan persyaratan SMKI.

7.4 Komunikasi

Organisasi harus menentukan kebutuhan berkomunikasi internal dan eksternal yang relevan dengan SMKI yang mencakup:

a) apa yang dikomunikasikan;

b) kapan dikomunikasikan;

c) dengan siapa dikomunikasikan;

d) siapa yang harus mengomunikasikan; dan

e) proses yang dipengaruhi oleh komunikasi tersebut.

7.5 Informasi terdokumentasi

7.5.1 Umum

Organisasi SMKI harus mencakup:

a) informasi terdokumentasi yang disyaratkan oleh Standar ini; dan

b) informasi terdokumentasi yang ditentukan oleh organisasi, sesuai yang diperlukan untuk efektivitas SMKI.

CATATAN cakupan informasi terdokumentasi untuk SMKI dapat berbeda antara satu organisasi dengan organisasi yang lain karena:

1) ukuran organisasi dan jenis kegiatan, proses, produk dan layanannya;

2) kompleksitas proses dan interaksinya; dan

3) kompetensi personelnya.

7.5.2 Membuat dan memperbarui

Ketika membuat dan memperbarui informasi terdokumentasi organisasi harus memastikan kecukupan hal-hal berikut ini:

a) identifikasi dan deskripsi (misal judul, tanggal, penulis, atau nomor referensi);

b) format (misal bahasa, versi perangkat lunak, grafis) dan media (misal kertas, elektronik); dan

c) reviu dan persetujuan untuk kesesuaian dan kecukupan.

3.5.1 7.5.3 Pengendalian informasi terdokumentasi

Informasi terdokumentasi yang dibutuhkan oleh SMKI dan Standar ini harus dikendalikan untuk memastikan:

a) informasi terdokumentasi tersedia dan cocok untuk digunakan, di mana dan kapan saja diperlukan; dan

b) informasi terdokumentasi cukup terlindungi (misal dari terungkapnya kerahasiaan, penyalahgunaan, atau hilangnya integritas).

Untuk pengendalian informasi terdokumentasi, organisasi harus menangani kegiatan-kegiatan berikut, jika dapat diterapkan:

c) distribusi, akses, pengambilan dan penggunaan;

d) penyimpanan dan pemeliharaan, termasuk pemeliharaan keterbacaan *(legibility)*;

e) pengendalian perubahan, misal pengendalian versi *(version control)*; dan

f) retensi (*retention*) dan disposisi *(disposition)*.

Informasi terdokumentasi yang bersumber dari luar, yang menurut organisasi diperlukan untuk perencanaan dan operasi SMKI, harus diidentifikasi kesesuaiannya dan dikendalikan.

CATATAN Akses mencakup keputusan terkait izin dan kewenangan untuk melihat informasi terdokumentasi saja, atau melihat dan mengubah informasi terdokumentasi, dll.

8 Operasi

8.1 Perencanaan dan pengendalian operasional

Organisasi harus merencanakan, menerapkan dan mengendalikan proses yang diperlukan untuk memenuhi persyaratan keamanan informasi, dan untuk menerapkan tindakan yang ditentukan dalam 6.1. Organisasi juga harus menerapkan rencana untuk mencapai sasaran keamanan informasi yang ditentukan dalam 6.2.

Organisasi harus menyimpan informasi terdokumentasi selama yang diperlukan untuk memiliki keyakinan bahwa proses telah dilakukan seperti yang direncanakan.

Organisasi harus mengendalikan perubahan yang direncanakan dan mereviu konsekuensi dari perubahan yang tidak diinginkan, mengambil tindakan seperlunya untuk mengurangi efek buruk.

Organisasi harus memastikan bahwa proses yang dialih dayakan telah ditetapkan dan dikendalikan.

8.2 Penilaian risiko keamanan informasi

Organisasi harus melakukan penilaian risiko keamanan informasi pada selang waktu terencana atau ketika perubahan signifikan diusulkan atau terjadi, dengan mempertimbangkan kriteria yang ditetapkan dalam 6.1.2 a).

Organisasi harus menyimpan informasi terdokumentasi dari hasil penilaian risiko keamanan informasi.

8.3 Penanganan risiko keamanan informasi

Organisasi harus menerapkan rencana penanganan risiko keamanan informasi.

Organisasi harus menyimpan informasi terdokumentasi hasil penanganan risiko keamanan informasi.

9 Evaluasi kinerja

9.1 Pemantauan, pengukuran, analisis dan evaluasi

Organisasi harus mengevaluasi kinerja keamanan informasi dan efektivitas SMKI.

Organisasi harus menentukan:

a) apa yang perlu dipantau dan diukur, termasuk proses dan pengendalian keamanan informasi;

b) metode untuk pemantauan, pengukuran, analisis dan evaluasi, jika dapat diterapkan, untuk memastikan hasil yang valid;

CATATAN Metode yang dipilih harus menghasilkan hasil yang dapat dibandingkan dan dapat diproduksi ulang untuk dinyatakan valid.

c) kapan pemantauan dan pengukuran harus dilakukan;

d) siapa yang harus memantau dan mengukur;

e) kapan hasil dari pemantauan dan pengukuran harus dianalisis dan dievaluasi; dan

f) siapa yang harus menganalisis dan mengevaluasi hasil tersebut.

Organisasi harus menyimpan informasi terdokumentasi yang memadai sebagai bukti hasil pemantauan dan pengukuran.

9.2 Audit internal

Organisasi harus melakukan audit internal pada selang waktu terencana untuk memberikan informasi apakah SMKI:

a) sesuai dengan

   1) persyaratan yang ditetapkan organisasi untuk SMKI-nya; dan

   2) persyaratan Standar ini;

b) diimplementasikan dan dipelihara secara efektif.

Organisasi harus:

c) merencanakan, menetapkan, menerapkan dan memelihara program audit, termasuk frekuensi, metode, tanggung jawab, persyaratan perencanaan dan pelaporan. Program audit harus mempertimbangkan pentingnya proses yang bersangkutan dan hasil audit sebelumnya;

d) menentukan kriteria audit dan ruang lingkup untuk setiap audit;

e) memilih auditor dan melakukan audit yang menjamin objektivitas dan ketidakberpihakan proses audit;

f) memastikan bahwa hasil audit tersebut dilaporkan kepada manajemen yang relevan; dan

g) menyimpan informasi terdokumentasi sebagai alat bukti dari program audit dan hasil audit.

9.3 Reviu manajemen

Manajemen puncak harus mereviu organisasi SMKI pada selang waktu terencana untuk memastikan kesesuaian, kecukupan dan efektivitas.

Reviu manajemen harus mencakup pertimbangan:

a) status tindakan dari reviu manajemen sebelumnya;

b) perubahan isu eksternal dan internal yang relevan dengan SMKI;

c) umpan balik dari kinerja keamanan informasi, termasuk kecenderungan dalam hal:

   1) ketidaksesuaian dan tindakan korektif;

   2) hasil pemantauan dan pengukuran;

   3) hasil audit; dan

   4) pemenuhan terhadap sasaran keamanan informasi;

d) umpan balik dari pihak yang berkepentingan;

e) hasil penilaian risiko dan status rencana penanganan risiko; dan

f) peluang untuk perbaikan berkelanjutan.

Keluaran dari reviu manajemen harus mencakup keputusan yang berkaitan dengan peluang perbaikan berkelanjutan dan setiap kebutuhan untuk perubahan SMKI.

Organisasi harus menyimpan informasi terdokumentasi sebagai bukti hasil reviu manajemen.

10 Perbaikan

10.1 Ketidaksesuaian dan tindakan korektif

Jika terjadi ketidaksesuaian, organisasi harus:

a) bereaksi terhadap ketidaksesuaian, dan jika dapat diterapkan:

   1) mengambil tindakan untuk mengendalikan dan mengoreksinya; dan

2) menangani konsekuensinya;

b) mengevaluasi kebutuhan tindakan untuk menghilangkan penyebab ketidaksesuaian, agar hal itu tidak terulang atau terjadi di tempat lain, dengan cara:

  1) mereviu ketidaksesuaian;

  2) menentukan penyebab ketidaksesuaian; dan

  3) menentukan apakah ada ketidaksesuaian serupa, atau berpotensi terjadi kembali;

c) melaksanakan tindakan apapun yang diperlukan;

d) mereviu efektivitas tindakan korektif apapun yang diambil; dan

e) membuat perubahan pada SMKI, jika diperlukan.

Tindakan korektif harus sesuai dengan efek dari ketidaksesuaian yang ditemui.

Organisasi harus menyimpan informasi terdokumentasi sebagai bukti dari:

f) sifat ketidaksesuaian dan tindakan berikutnya yang diambil, dan

g) hasil dari setiap tindakan korektif.

10.2 Perbaikan berkelanjutan

Organisasi harus terus memperbaiki kesesuaian, kecukupan dan efektivitas SMKI.

Lampiran A
(normatif)
Acuan untuk sasaran kendali dan kendali

Sasaran kendali dan kendali yang tercantum dalam Tabel A.1 secara langsung berasal dari dan sesuai dengan yang terdaftar di ISO/IEC 27002:2013[1], Klausul 5 hingga klausul 18, dan akan dipergunakan dalam Klausul 6.1.3.

Tabel A.1 — Sasaran kendali dan kendali

A.5 Kebijakan keamanan informasi		
A.5.1 Arahan manajemen untuk keamanan informasi		
Sasaran: Untuk memberikan arah dan dukungan manajemen untuk keamanan informasi sesuai dengan persyaratan bisnis dan regulasi dan hukum yang relevan		
A.5.1.1	Kebijakan untuk keamanan informasi	*Kendali* Seperangkat kebijakan untuk keamanan informasi harus ditetapkan, disetujui oleh manajemen, diterbitkan dan dikomunikasikan kepada karyawan dan pihak luar yang terkait.
A.5.1.2	Reviu kebijakan keamanan informasi	*Kendali* Kebijakan untuk keamanan informasi harus direviu pada interval waktu terencana atau jika terjadi perubahan signifikan untuk memastikan kesesuaian, kecukupan dan keefektifan yang berkelanjutan
A.6 Organisasi keamanan informasi		
A.6.1 Organisasi internal		
Sasaran: Untuk membentuk kerangka kerja manajemen untuk memulai dan mengendalikan implementasi dan operasi keamanan informasi dalam organisasi.		
A.6.1.1	Peran dan tanggung jawab keamanan informasi	*Kendali* Semua tanggung jawab keamanan informasi harus didefinisikan dan dialokasikan.
A.6.1.2	Pemisahan tugas	*Kendali* Tugas dan area tanggung jawab yang bertentangan harus dipisahkan (dijabat oleh personel yang berbeda) untuk mengurangi kemungkinan dari modifikasi yang tidak sah atau tidak sengaja atau penyalahgunaan aset organisasi.
A.6.1.3	Hubungan dengan pihak berwenang	*Kendali* Hubungan baik dengan pihak berwenang terkait harus dipelihara.
A.6.1.4	Hubungan dengan kelompok minat khusus	*Kendali* Hubungan baik dengan komunitas, forum, dan asosiasi profesional spesialis keamanan harus dipelihara.

Tabel A.1 - (lanjutan)

A.6.1.5	Keamanan informasi dalam manajemen proyek	*Kendali* Keamanan informasi harus diterapkan ke dalam manajemen proyek, tanpa memperhatikan tipe proyeknya.
A.6.2 Perangkat bergerak (*mobile device*) dan *teleworking*		
Sasaran: Untuk menjamin keamanan *teleworking* dan penggunaan perangkat bergerak		
A.6.2.1	Kebijakan perangkat bergerak	*Kendali* Kebijakan dan tindakan keamanan yang mendukung harus diadopsi untuk mengelola risiko yang terjadi akibat dari penggunaan perangkat bergerak.
A.6.2.2	*Teleworking*	*Kendali* Kebijakan dan tindakan keamanan yang mendukung harus diimplementasikan untuk melindungi informasi yang diakses, diproses atau disimpan di dalam situs *teleworking*.
A.7 Keamanan sumber daya manusia		
A.7.1 Sebelum dipekerjakan		
Sasaran: Untuk memastikan bahwa karyawan dan kontraktor memahami tanggung jawab mereka dan sesuai dengan peran yang ditetapkan bagi mereka.		
A.7.1.1	Penyaringan	*Kendali* Verifikasi latar belakang dari semua calon pegawai harus dilaksanakan berdasarkan hukum, regulasi dan etika terkait dan harus proporsional terhadap persyaratan bisnis, klasifikasi informasi yang akan diakses, dan risiko yang dipersepsikan.
A.7.1.2	Syarat dan ketentuan kepegawaian	*Kendali* Perjanjian tertulis dengan pegawai dan kontraktor harus menyatakan tanggung jawab keamanan informasi mereka dan organisasi.
A.7.2 Selama bekerja		
Sasaran: Untuk memastikan bahwa pegawai dan kontraktor menyadari dan memenuhi tanggung jawab keamanan informasi mereka		
A.7.2.1	Tanggung jawab manajemen	*Kendali* Manajemen harus mewajibkan semua pegawai dan kontraktor menerapkan keamanan informasi berdasarkan kebijakan dan prosedur organisasi yang sudah ditetapkan.
A.7.2.2	Kepedulian, pendidikan, dan pelatihan keamanan informasi	*Kendali* Semua pegawai organisasi dan kontraktor (jika relevan) harus menerima kepedulian, pendidikan, dan pelatihan yang memadai dan pemberitahuan secara berkala mengenai kebijakan dan prosedur organisasi, sesuai dengan fungsi kerja mereka.

Tabel A.1 - (lanjutan)

A.7.2.3	Proses pendisiplinan	*Kendali* Harus ada proses pendisiplinan yang resmi dan terkomunikasikan terhadap penindakan pegawai yang melakukan pelanggaran keamanan informasi.
A.7.3 Penghentian dan perubahan kepegawaian		
Sasaran: Untuk melindungi kepentingan organisasi sebagai bagian dari proses pengubahan atau penghentian kepegawaian.		
A.7.3.1	Penghentian atau perubahan tanggung jawab kepegawaian	*Kendali* Setelah penghentian atau perubahan kepegawaian, tugas dan tanggung jawab keamanan informasi yang masih berlaku harus ditetapkan, dikomunikasikan kepada pegawai atau kontraktor, dan ditegakkan.
A.8 Manajemen aset		
A.8.1 Tanggung jawab terhadap aset		
Sasaran: Untuk mengenali aset organisasi dan menetapkan tanggung jawab perlindungan yang sesuai.		
A.8.1.1	Inventaris aset	*Kendali* Aset yang berhubungan dengan informasi dan fasilitas pengolahan informasi harus diidentifikasi dan inventaris dari aset-aset ini harus dicatat dan dipelihara.
A.8.1.2	Kepemilikan aset	*Kendali* Aset yang dipelihara dalam inventaris harus dimiliki (ada personel yang bertanggung jawab).
A.8.1.3	Penggunaan yang dapat diterima (*acceptable use*) atas aset	*Kendali* Aturan untuk penggunaan yang dapat diterima atas informasi dan aset yang berhubungan dengan informasi dan fasilitas pengolahan informasi harus diidentifikasi, didokumentasi dan diimplementasikan.
A.8.1.4	Pengembalian aset	*Kendali* Semua pegawai dan pengguna pihak eksternal harus mengembalikan semua aset organisasi yang dikuasainya ketika terjadi penghentian kepegawaian, kontrak atau perjanjian mereka.
A.8.2 Klasifikasi informasi		
Sasaran: Untuk memastikan bahwa informasi mendapatkan tingkat perlindungan yang layak berdasarkan kepentingannya di dalam organisasi.		
A.8.2.1	Klasifikasi informasi	*Kendali* Informasi harus diklasifikasikan sesuai persyaratan hukum, nilai, kekritisan dan kerentanan terhadap penyingkapan atau modifikasi yang tidak sah.

Tabel A.1 - (lanjutan)

A.8.2.2	Pelabelan informasi	*Kendali* Seperangkat prosedur yang tepat untuk pelabelan informasi harus dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi oleh organisasi.
A.8.2.3	Penanganan aset	*Kendali* Prosedur penanganan aset harus dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi organisasi.
A.8.3 Penanganan media		
Sasaran: Untuk mencegah penyingkapan, modifikasi, pemindahan atau penghancuran tidak sah terhadap informasi yang disimpan di dalam media.		
A.8.3.1	Manajemen media yang dapat dipindahkan (*removable media*)	*Kendali* Prosedur harus diimplementasikan untuk manajemen media yang dapat dipindahkan sesuai dengan skema klasifikasi yang diadopsi organisasi.
A.8.3.2	Pembuangan media	*Kendali* Media harus dihancurkan dengan aman saat tidak lagi dibutuhkan, dengan menggunakan prosedur baku.
A.8.3.3	Perpindahan media secara fisik	*Kendali* Media yang mengandung informasi harus dilindungi terhadap akses, penyalahgunaan, atau perubahan yang tidak sah selama dipindahkan.
A.9 Kendali akses		
A.9.1 Persyaratan bisnis untuk kendali akses		
Sasaran: Untuk membatasi akses ke informasi dan fasilitas pengolahan informasi.		
A.9.1.1	Kebijakan kendali akses	*Kendali* Kebijakan kendali akses harus ditetapkan, didokumentasikan, dan direviu berdasarkan dan persyaratan bisnis dan keamanan informasi.
A.9.1.2	Akses ke jaringan dan layanan jaringan	*Kendali* Pengguna hanya akan disediakan akses ke jaringan dan layanan jaringan yang telah secara khusus diberi wewenang untuk digunakan.
A.9.2 Manajemen akses pengguna		
Sasaran: Untuk memastikan akses pengguna yang berwenang dan untuk mencegah akses oleh pihak yang tidak berwenang ke sistem dan layanan.		
A.9.2.1	Registrasi dan pembatalan registrasi pengguna	*Kendali* Proses registrasi dan pembatalan registrasi pengguna yang resmi harus diimplementasikan untuk mengaktifkan penetapan hak akses.

Tabel A.1 - (lanjutan)

A.9.2.2	Penyediaan akses pengguna	*Kendali* Proses penyediaan akses pengguna yang resmi harus diimplementasikan untuk menetapkan atau mencabut hak akses untuk semua tipe pengguna ke semua sistem dan layanan.
A.9.2.3	Manajemen hak akses istimewa	*Kendali* Pengalokasian dan penggunaan hak akses istimewa harus dibatasi dan dikendalikan.
A.9.2.4	Manajemen informasi otentikasi rahasia dari pengguna	*Kendali* Alokasi dari informasi otentikasi rahasia harus dikendalikan melalui proses manajemen yang resmi.
A.9.2.5	Reviu hak akses pengguna	*Kendali* Pemilik aset harus mereviu hak akses pengguna secara periodik.
A.9.2.6	Penghapusan atau penyesuaian hak akses	*Kendali* Hak akses semua pegawai dan pengguna pihak eksternal pada informasi dan fasilitas pengolahan informasi harus dihapus sewaktu terjadi penghentian kepegawaian, kontrak atau perjanjian mereka, atau disesuaikan atas perubahan yang terjadi.
A.9.3 Tanggung jawab pengguna		
Sasaran: Untuk membuat pengguna bertanggung jawab dalam menjaga informasi otentikasi mereka.		
A.9.3.1	Penggunaan informasi otentikasi rahasia	*Kendali* Pengguna harus disyaratkan mengikuti praktik organisasi dalam penggunaan informasi otentikasi rahasia.
A.9.4 Kendali akses sistem dan aplikasi		
Sasaran: Untuk mencegah akses oleh pihak yang tidak sah ke sistem dan aplikasi.		
A.9.4.1	Pembatasan akses informasi	*Kendali* Akses ke informasi dan fungsi sistem aplikasi harus dibatasi sesuai dengan kebijakan kendali akses.
A.9.4.2	Prosedur *log-on* yang aman	*Kendali* Ketika disyaratkan oleh kebijakan pengendalian akses, akses ke sistem dan aplikasi harus dikendalikan oleh prosedur *log-on* yang aman.
A.9.4.3	Sistem manajemen kata kunci *(password)*	*Kendali* Sistem manajemen kata kunci harus interaktif dan menjamin kualitas kata kunci.

Tabel A.1 - (lanjutan)

A.9.4.4	Penggunaan program utilitas istimewa	*Kendali* Penggunaan program utilitas yang mungkin mampu membatalkan kendali sistem dan aplikasi harus dibatasi dan dikendalikan secara ketat.
A.9.4.5	Kendali akses ke kode sumber program	*Kendali* Akses ke kode sumber program harus dibatasi.
A.10 Kriptografi		
A.10.1 Kendali kriptografi		
Sasaran: Untuk memastikan penggunaan kriptografi secara tepat dan efektif dalam melindungi kerahasiaan (*confidentiality*), keotentikkan (*authenticity*) dan/atau keutuhan (*integrity*) informasi.		
A.10.1.1	Kebijakan terhadap penggunaan kendali kriptografi	*Kendali* Kebijakan terhadap penggunaan kendali kriptografi untuk perlindungan informasi harus dikembangkan dan diimplementasikan.
A.10.1.2	Manajemen kunci	*Kendali* Kebijakan terhadap penggunaan, perlindungan dan masa hidup kunci kriptografi harus dikembangkan dan diimplementasikan dalam keseluruhan siklus hidupnya.
A.11 Keamanan fisik dan lingkungan		
A.11.1 Daerah aman		
Sasaran: Untuk mencegah akses fisik yang tidak sah, kerusakan dan interferensi terhadap informasi dan fasilitas pengolahan informasi organisasi.		
A.11.1.1	Batas fisik *(perimeter)* keamanan	*Kendali* Batas fisik keamanan harus ditetapkan dan digunakan untuk melindungi area yang mengandung informasi dan fasilitas pengolahan informasi yang sensitif atau kritis.
A.11.1.2	Kendali masuk fisik	*Kendali* Daerah aman harus dilindungi oleh kendali masuk yang sesuai untuk menjamin hanya personel berwenang saja yang diizinkan untuk mengakses.
A.11.1.3	Mengamankan kantor, ruangan dan fasilitas	*Kendali* Keamanan fisik untuk kantor, ruangan dan fasilitas harus dirancang dan diterapkan.
A.11.1.4	Melindungi terhadap ancaman eksternal dan lingkungan	*Kendali* Perlindungan fisik terhadap bencana alam, serangan jahat atau kecelakaan harus dirancang dan diterapkan.
A.11.1.5	Bekerja dalam daerah aman	*Kendali* Prosedur untuk bekerja dalam daerah aman harus dirancang dan diterapkan.

Tabel A.1 - (lanjutan)

A.11.1.6	Daerah pengiriman dan bongkar muat	*Kendali* Titik akses seperti area bongkar muat dan titik lain yang dapat dimasuki orang yang tidak berwenang harus dikendalikan dan, jika mungkin, dipisahkan dari fasilitas pengolahan informasi untuk mencegah akses oleh pihak yang tidak berwenang
A.11.2 Peralatan		
Sasaran: Untuk mencegah kerugian, kerusakan, pencurian, atau penguasaan tanpa hak (*compromise*) aset dan gangguan terhadap operasi organisasi.		
A.11.2.1	Penempatan dan perlindungan peralatan	*Kendali* Peralatan harus ditempatkan dan dilindungi untuk mengurangi risiko dari ancaman dan bahaya lingkungan, dan peluang untuk akses oleh pihak yang tidak berwenang.
A.11.2.2	Utilitas pendukung	*Kendali* Peralatan harus dilindungi dari kegagalan catu daya dan gangguan lain yang disebabkan kegagalan utilitas pendukung.
A.11.2.3	Keamanan kabel	*Kendali* Kabel daya dan telekomunikasi yang membawa data atau layanan informasi pendukung harus dilindungi dari pencegatan, interferensi atau kerusakan.
A.11.2.4	Pemeliharaan peralatan	*Kendali* Peralatan harus dipelihara secara tepat untuk menjamin ketersediaan yang berkelanjutan dan integritas
A.11.2.5	Pemindahan aset	*Kendali* Peralatan, informasi atau perangkat lunak tidak boleh dibawa keluar lokasi tanpa izin yang berwenang
A.11.2.6	Keamanan dari peralatan dan aset di luar lokasi *(off-premises)*	*Kendali* Keamanan harus diterapkan untuk aset di luar kantor dengan memperhitungkan risiko yang berbeda akibat bekerja di luar lokasi organisasi.
A.11.2.7	Pembuangan atau penggunaan kembali peralatan secara aman	*Kendali* Semua peralatan yang mengandung media penyimpanan harus diverifikasi untuk menjamin bahwa data rahasia dan perangkat lunak berlisensi apapun sudah dihapus atau ditimpa secara aman sebelumnya untuk dibuang atau dipergunakan kembali.
A.11.2.8	Peralatan pengguna yang tidak diawasi	*Kendali* Pengguna harus menjamin bahwa peralatan yang tidak diawasi memiliki perlindungan yang layak.

Tabel A.1 - (lanjutan)

A.11.2.9	Kebijakan mengosongkan meja dan mengosongkan layar	*Kendali* Kebijakan mengosongkan meja dari kertas dan media penyimpanan yang dapat dipindah dan kebijakan mengosongkan layar dari fasilitas pengolahan informasi harus diadopsi.
A.12 Keamanan operasi		
A.12.1 Prosedur dan tanggung jawab operasional		
Sasaran: Untuk menjamin operasi fasilitas pengolahan informasi benar dan aman.		
A.12.1.1	Prosedur operasional yang didokumentasikan	*Kendali* Prosedur operasional harus didokumentasikan dan tersedia untuk semua pengguna yang membutuhkannya.
A.12.1.2	Manajemen perubahan	*Kendali* Perubahan terhadap organisasi, proses bisnis, fasilitas pengolahan informasi dan sistem yang mempengaruhi keamanan informasi harus dikendalikan.
A.12.1.3	Manajemen kapasitas	*Kendali* Penggunaan sumber daya harus diawasi, diatur dan dibuat proyeksi atas kebutuhan kapasitas di masa datang untuk memastikan performa sistem yang dibutuhkan.
A.12.1.4	Pemisahan lingkungan pengembangan, pengujian dan operasional	*Kendali* Lingkungan pengembangan, pengujian, dan operasional harus dipisahkan untuk mengurangi risiko akses atau perubahan tidak sah pada lingkungan operasional
A.12.2 Perlindungan dari *malware*		
Sasaran: Untuk memastikan informasi dan fasilitas pengolahan informasi terlindungi dari *malware*.		
A.12.2.1	Kendali terhadap *malware*	*Kendali* Kendali deteksi, pencegahan dan pemulihan untuk melindungi terhadap *malware* harus diimplementasikan, digabungkan dengan kepedulian pengguna yang sesuai.
A.12.3 Cadangan (*Backup*)		
Sasaran: Untuk melindungi dari kehilangan data		
A.12.3.1	Cadangan informasi	*Kendali* Salinan cadangan informasi, perangkat lunak dan *image* sistem harus diambil dan diuji secara berkala sesuai dengan kebijakan cadangan yang disetujui.

Tabel A.1 - (lanjutan)

A.12.4 Pencatatan *(logging)* dan pemantauan		
Sasaran: Untuk mencatat peristiwa dan menghasilkan barang bukti.		
A.12.4.1	Pencatatan kejadian *(event logging)*	*Kendali* Catatan kejadian yang merekam aktivitas pengguna, pengecualian (*exception*), kegagalan dan kejadian keamanan informasi harus diciptakan, disimpan dan direviu secara berkala.
A.12.4.2	Perlindungan terhadap informasi *log*	*Kendali* Fasilitas untuk mencatat log dan informasi *log* harus dilindungi terhadap pemalsuan dan akses yang tidak berwenang.
A.12.4.3	*Log* administrator dan operator	*Kendali* Aktivitas administrator sistem dan operator sistem harus dicatat dan catatan tersebut dilindungi dan direviu secara berkala .
A.12.4.4	Sinkronisasi waktu	*Kendali* Waktu dari semua sistem pengolahan informasi yang terkait dalam organisasi atau wilayah keamanan harus disinkronisasikan ke sumber waktu acuan tunggal.
A.12.5 Kendali perangkat lunak operasional		
Sasaran: Untuk memastikan integritas sistem operasional.		
A.12.5.1	Instalasi perangkat lunak pada sistem operasional	*Kendali* Prosedur harus diimplementasikan untuk mengendalikan instalasi perangkat lunak pada sistem operasional.
A.12.6 Manajemen kerentanan teknis		
Sasaran: Untuk mencegah eksploitasi kerentanan teknis.		
A.12.6.1	Manajemen kerentanan teknis	*Kendali* Informasi mengenai kerentanan teknis sistem informasi yang digunakan harus diperoleh tepat waktu, keterpaparan (*exposure*) organisasi terhadap kerentanan tersebut dievaluasi dan tindakan yang tepat diambil untuk mengatasi risiko terkait.
A.12.6.2	Pembatasan terhadap instalasi perangkat lunak	*Kendali* Aturan yang mengatur instalasi perangkat lunak oleh pengguna harus ditetapkan dan diimplementasikan.

Tabel A.1 - (lanjutan)

A.12.7 Pertimbangan audit sistem informasi		
Sasaran: Untuk meminimalkan dampak dari aktivitas audit sistem operasional.		
A.12.7.1	Kendali audit sistem informasi	*Kendali* Persyaratan dan aktivitas audit yang melibatkan verifikasi sistem operasional harus direncanakan secara hati-hati dan disepakati untuk memperkecil gangguan ke proses bisnis.
A.13 Keamanan komunikasi		
A.13.1 Manajemen keamanan jaringan		
Sasaran: Untuk menjamin perlindungan informasi dalam jaringan dan fasilitas pendukung pengolahan informasi.		
A.13.1.1	Kendali jaringan	*Kendali* Jaringan harus dikelola dan dikendalikan untuk melindungi informasi dalam sistem dan aplikasi.
A.13.1.2	Keamanan layanan jaringan	*Kendali* Mekanisme keamanan, tingkat layanan dan persyaratan manajemen dari semua layanan jaringan harus diidentifikasi dan dimasukkan dalam perjanjian layanan jaringan yang dapat dikerjakan sendiri atau dialihdayakan.
A.13.1.3	Pemisahan dalam jaringan	*Kendali* Kelompok layanan informasi, pengguna dan sistem informasi harus dipisahkan pada jaringan.
A.13.2 Perpindahan informasi		
Sasaran: Untuk memelihara keamanan informasi yang dipindahkan dalam suatu organisasi ataupun dengan pihak luar.		
A.13.2.1	Prosedur dan kebijakan perpindahan informasi	*Kendali* Kebijakan, prosedur dan kendali perpindahan yang resmi harus ada untuk melindungi perpindahan informasi melalui penggunaan semua jenis fasilitas komunikasi.
A.13.2.2	Perjanjian perpindahan informasi	*Kendali* Perjanjian harus mengatur perpindahan informasi bisnis yang aman antara organisasi dan pihak eksternal.
A.13.2.3	Pesan elektronik	*Kendali* Informasi yang terdapat dalam pesan elektronik harus dilindungi dengan tepat.
A.13.2.4	Perjanjian kerahasiaan atau menjaga rahasia (*nondisclosure agreement*)	*Kendali* Persyaratan untuk perjanjian kerahasiaan atau menjaga rahasia mencerminkan kebutuhan organisasi untuk perlindungan informasi harus diidentifikasi, direviu secara teratur dan didokumentasikan.

Tabel A.1 - (lanjutan)

A.14 Akuisisi, pengembangan dan perawatan sistem		
A.14.1 Persyaratan keamanan sistem informasi		
Sasaran: Untuk memastikan bahwa keamanan informasi merupakan sebuah bagian integral dari sistem informasi di keseluruhan daur hidup. Hal ini juga termasuk persyaratan untuk sistem informasi yang menyediakan layanan melalui jaringan publik.		
A.14.1.1	Analisis dan spesifikasi persyaratan keamanan informasi	*Kendali* Persyaratan yang terkait keamanan informasi harus termasuk dalam persyaratan untuk sistem informasi baru atau pengembangan sistem informasi yang ada.
A.14.1.2	Pengamanan layanan aplikasi pada jaringan publik	*Kendali* Informasi yang terdapat dalam layanan aplikasi yang melewati jaringan publik harus dilindungi dari aktivitas yang bersifat menipu, perselisihan kontrak, dan pembukaan rahasia dan modifikasi secara tidak sah.
A.14.1.3	Perlindungan transaksi layanan aplikasi	*Kendali* Informasi yang terdapat di dalam transaksi layanan aplikasi harus dilindungi untuk mencegah transmisi yang tidak lengkap, pemilihan jalur yang salah (mis-routing), pengubahan pesan yang tidak sah, pembukaan rahasia yang tidak sah, duplikasi atau balasan pesan yang tidak sah.
A.14.2 Keamanan dalam proses pengembangan dan dukungan		
Sasaran: Untuk memastikan bahwa keamanan informasi dirancang dan diterapkan dalam daur hidup pengembangan sistem informasi.		
A.14.2.1	Kebijakan pengembangan yang aman	*Kendali* Aturan untuk pengembangan perangkat lunak dan sistem harus ditetapkan dan diterapkan untuk pengembangan dalam organisasi.
A.14.2.2	Prosedur kendali perubahan sistem	*Kendali* Perubahan terhadap sistem dalam daur hidup pengembangan harus dikendalikan dengan penggunaan prosedur kendali perubahan yang baku.
A.14.2.3	Reviu teknis aplikasi setelah perubahan *platform* operasi	*Kendali* Ketika *platform* operasi diubah, aplikasi kritis bisnis harus direviu dan diuji untuk memastikan tidak adanya dampak yang merugikan pada operasi atau keamanan organisasi.
A.14.2.4	Pembatasan dalam pengubahan paket perangkat lunak	*Kendali* Modifikasi pada paket perangkat lunak harus dicegah, dibatasi untuk perubahan yang diperlukan, dan semua perubahan harus dikendalikan dengan ketat.

Tabel A.1 - (lanjutan)

A.14.2.5	Prinsip rekayasa sistem yang aman	*Kendali* Prinsip untuk rekayasa sistem yang aman harus ditetapkan, didokumentasikan, dipertahankan dan diterapkan ke setiap upaya implementasi sistem informasi.
A.14.2.6	Lingkungan pengembangan yang aman	*Kendali* Organisasi harus membangun dan melindungi secara memadai lingkungan pengembangan yang aman untuk upaya pengembangan dan integrasi sistem yang mencakup seluruh daur hidup pengembangan sistem.
A.14.2.7	Pengembangan oleh alihdaya	*Kendali* Organisasi harus mengawasi dan memantau aktivitas pengembangan sistem yang dialihdayakan.
A.14.2.8	Pengujian keamanan sistem	*Kendali* Pengujian fungsi keamanan harus dilakukan selama pengembangan.
A.14.2.9	Pengujian penerimaan sistem	*Kendali* Program pengujian penerimaan dan kriteria terkait harus ditetapkan untuk sistem informasi baru, peningkatan dan versi baru.
A.14.3 Data uji		
Sasaran: Untuk memastikan perlindungan terhadap data yang digunakan untuk pengujian.		
A.14.3.1	Proteksi data uji	*Kendali* Data uji harus dipilih dengan hati-hati, dilindungi, dan dikendalikan.
A.15 Hubungan pemasok		
A.15.1 Keamanan informasi dalam hubungan pemasok		
Sasaran: Untuk memastikan perlindungan dari aset organisasi yang dapat diakses oleh pemasok.		
A.15.1.1	Kebijakan keamanan informasi untuk hubungan pemasok	*Kendali* Persyaratan keamanan informasi untuk mitigasi risiko yang berkaitan dengan akses pemasok untuk aset organisasi harus disetujui dengan pemasok dan didokumentasikan.
A.15.1.2	Memasukkan klausul keamanan dalam perjanjian pemasok	*Kendali* Semua persyaratan keamanan informasi yang relevan harus ditetapkan dan disetujui dengan setiap pemasok yang dapat mengakses, memroses, menyimpan, berkomunikasi, atau menyediakan komponen infrastruktur TI untuk informasi organisasi.

Tabel A.1 - (lanjutan)

A.15.1.3	Rantai pasok teknologi informasi dan komunikasi	*Kendali* Perjanjian dengan pemasok harus termasuk persyaratan untuk mengatasi risiko keamanan informasi terkait rantai pasok layanan dan produk teknologi informasi dan komunikasi.
A.15.2 Manajemen penyampaian layanan pemasok		
Sasaran: Untuk menjaga tingkat yang disetujui dari keamanan informasi dan penyampaian layanan dijalankan sesuai dengan yang terdapat dalam perjanjian pemasok.		
A.15.2.1	Pemantauan dan reviu layanan pemasok	*Kendali* Organisasi harus secara teratur memantau, mereviu dan mengaudit penyampaian layanan pemasok..
A.15.2.2	Mengelola perubahan layanan pemasok	*Kendali* Perubahan ketentuan layanan oleh pemasok, termasuk mempertahankan dan meningkatkan kebijakan, prosedur dan kendali keamanan informasi yang ada harus dikelola dengan memperhitungkan tingkat kekritisan informasi, sistem dan proses bisnis yang terlibat, dan asesmen ulang terhadap risiko.
A.16 Manajemen insiden keamanan informasi		
A.16.1 Manajemen insiden keamanan informasi dan perbaikan		
Sasaran: Untuk memastikan pendekatan konsisten dan efektif untuk menajemen insiden keamanan informasi, termasuk komunikasi tentang kejadian dan kelemahan keamanan.		
A.16.1.1	Tanggung jawab dan prosedur	*Kendali* Tanggung jawab dan prosedur manajemen harus ditetapkan untuk memastikan tanggapan yang cepat, efektif dan tepat untuk insiden keamanan informasi.
A.16.1.2	Pelaporan kejadian keamanan informasi	*Kendali* Kejadian keamanan informasi harus dilaporkan melalui saluran manajemen yang sesuai secepat mungkin.
A.16.1.3	Pelaporan kelemahan keamanan informasi	*Kendali* Karyawan dan kontraktor yang menggunakan sistem informasi dan layanan organisasi harus mencatat dan melaporkan kelemahan keamanan informasi yang diamati dan dicurigai dalam sistem atau layanan.
A.16.1.4	Asesmen dan keputusan pada kejadian keamanan informasi	*Kendali* Kejadian keamanan informasi harus dinilai dan harus diputuskan jika akan diklasifikasikan sebagai insiden keamanan informasi.

Tabel A.1 - (lanjutan)

A.16.1.5	Tanggapan terhadap insiden keamanan informasi	*Kendali* Insiden keamanan informasi harus ditanggapi sesuai dengan prosedur yang telah didokumentasikan..
A.16.1.6	Pembelajaran dari insiden keamanan informasi	*Kendali* Pengetahuan yang diperoleh dari menganalisis dan mengatasi insiden keamanan informasi harus digunakan untuk mengurangi kemungkinan insiden atau dampak insiden di masa depan.
A.16.1.7	Pengumpulan bukti	*Kendali* Organisasi harus mendefinisikan dan menetapkan prosedur untuk identifikasi, pengumpulan, akuisisi dan preservasi informasi, yang dapat berguna sebagai bukti.
A.17 Aspek keamanan informasi dari manajemen keberlangsungan bisnis		
A.17.1 Keberlangsungan keamanan informasi		
Sasaran: Keberlangsungan keamanan informasi harus ditanamkan dalam sistem manajemen keberlangsungan bisnis organisasi.		
A.17.1.1	Perencanaan keberlangsungan keamanan informasi	*Kendali* Organisasi harus menentukan persyaratannya untuk keamanan informasi dan keberlangsungan manajemen keamanan informasi dalam situasi yang merugikan, contoh selama krisis atau bencana.
A.17.1.2	Mengimplementasikan keberlangsungan keamanan informasi	*Kendali* Organisasi harus menetapkan, mendokumentasikan, menerapkan dan menjaga proses, prosedur, dan kendali untuk memastikan tingkat yang dibutuhkan dalam keberlangsungan keamanan informasi selama situasi yang merugikan.
A.17.1.3	Memeriksa, mereviu dan mengevaluasi keberlangsungan keamanan informasi	*Kendali* Organisasi harus memeriksa kendali keberlangsungan keamanan informasi yang ditetapkan dan diimplementasikan secara berkala untuk memastikan bahwa kendali tersebut valid dan efektif selama situasi yang merugikan.
A.17.2 Redundansi		
Sasaran: Untuk memastikan ketersediaan fasilitas pengolahan informasi.		
A.17.2.1	Ketersediaan fasilitas pengolahan informasi	*Kendali* Fasilitas pengolahan informasi harus diimplementasikan dengan redundansi yang cukup untuk memenuhi persyaratan ketersediaan.

Tabel A.1 - (lanjutan)

A.18 Kesesuaian		
A.18.1 Kesesuaian dengan persyaratan hukum dan kontraktual		
Sasaran: Untuk menghindari pelanggaran hukum, undang-undang, peraturan atau kewajiban kontraktual yang terkait dengan keamanan informasi dan persyaratan keamanan lainnya.		
A.18.1.1	Identifikasi persyaratan perundang-undangan dan kontraktual yang berlaku	*Kendali* Semua persyaratan undang-undang, peraturan, kontraktual yang relevan, dan pendekatan organisasi untuk memenuhi persyaratan ini, harus diidentifikasi secara eksplisit, didokumentasikan dan dijaga tetap mutakhir untuk setiap sistem informasi dan organisasi.
A.18.1.2	Hak kekayaan intelektual	*Kendali* Prosedur yang sesuai harus diimplementasikan untuk memastikan kesesuaian dengan persyaratan hukum dan perundang-undangan serta kontraktual yang terkait dengan hak atas kekayaan intelektual dan penggunaan produk perangkat lunak *proprietary*.
A.18.1.3	Perlindungan rekaman	*Kendali* Rekaman harus dilindungi dari kehilangan, kerusakan, pemalsuan, akses tidak sah dan rilis tidak sah, sesuai dengan persyaratan peraturan perundangan, kontraktual dan bisnis..
A.18.1.4	Privasi dan perlindungan atas informasi pribadi yang dapat diidentifikasikan	*Kendali* Privasi dan perlindungan informasi pribadi yang dapat diidentifikasikan harus dipastikan sebagaimana disyaratkan dalam peraturan perundangan yang relevan.
A.18.1.5	Peraturan kendali kriptografi	*Kendali* kendali kriptografi harus sesuai dengan semua peraturan perundangan dan perjanjian yang relevan.
A.18.2 Reviu keamanan informasi		
Sasaran: Untuk memastikan bahwa keamanan informasi diimplementasikan dan dioperasikan sesuai dengan kebijakan dan prosedur organisasi.		
A.18.2.1	Reviu independen terhadap keamanan informasi	*Kendali* Pendekatan organisasi untuk mengelola keamanan informasi dan implementasinya (contoh: sasaran kendali, kendali, kebijakan, proses dan prosedur untuk keamanan informasi) harus direviu berkala secara independen atau ketika terjadi perubahan signifikan.

Tabel A.1 - (lanjutan)

A.18.2.2	Kesesuaian dengan kebijakan dan standar keamanan	*Kendali* Manajer harus secara teratur mereviu kesesuaian prosedur dan pemrosesan informasi dalam area tanggung jawab mereka dengan kebijakan keamanan, standar dan persyaratan keamanan lainnya yang sesuai.
A.18.2.3	Reviu kesesuaian teknis	*Kendali* Sistem informasi harus direviu secara reguler agar tetap sesuai dengan kebijakan dan standar keamanan informasi organisasi.

Bibliografi

[1] ISO/IEC 27002:2013, *Information technology — Security Techniques — Code of practice for information security controls*

[2] ISO/IEC 27003, *Information technology — Security techniques — Information security management system implementation guidance*

[3] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Measurement*

[4] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[5] ISO 31000:2009, *Risk management — Principles and guidelines*

[6] *ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO, 2012*

Information technology – Security techniques – Information security management systems – Requirements

1 Scope

This Standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This Standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this Standard are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this Standard.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.3 of ISO 31000:2009[5].

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

a) interested parties that are relevant to the information security management system; and

b) the requirements of these interested parties relevant to information security.

NOTE The requirements of interested parties may include legal and regulatory requirements and contractual obligations.

4.3 Determining the scope of the information security management system

The organization shall determine the boundaries and applicability of the information security management system to establish its scope.

When determining this scope, the organization shall consider:
a) the external and internal issues referred to in 4.1;

b) the requirements referred to in 4.2; and

c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

The scope shall be available as documented information.

4.4 Information security management system

The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this Standard.

5 Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the information security management system by:

a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;

b) ensuring the integration of the information security management system requirements into the organization's processes;

c) ensuring that the resources needed for the information security management system are available;

d) communicating the importance of effective information security management and of conforming to the information security management system requirements;

e) ensuring that the information security management system achieves its intended outcome(s);

f) directing and supporting persons to contribute to the effectiveness of the information security management system;

g) promoting continual improvement; and

h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

5.2 Policy

Top management shall establish an information security policy that:

a) is appropriate to the purpose of the organization;

b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;

c) includes a commitment to satisfy applicable requirements related to information security; and

d) includes a commitment to continual improvement of the information security management system.

The information security policy shall:

a) be available as documented information;

b) be communicated within the organization; and

c) be available to interested parties, as appropriate.

5.3 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.

Top management shall assign the responsibility and authority for:

a) ensuring that the information security management system conforms to the requirements of this Standard; and

b) reporting on the performance of the information security management system to top management.

NOTE Top management may also assign responsibilities and authorities for reporting performance of the information security management system within the organization.

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

a) ensure the information security management system can achieve its intended outcome(s);

b) prevent, or reduce, undesired effects; and

c) achieve continual improvement.

The organization shall plan:

d) actions to address these risks and opportunities; and

e) how to

   1) integrate and implement the actions into its information security management system processes; and

   2) evaluate the effectiveness of these actions.

6.1.2 Information security risk assessment

The organization shall define and apply an information security risk assessment process that:

a) establishes and maintains information security risk criteria that include:

   1) the risk acceptance criteria; and

   2) criteria for performing information security risk assessments;

b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;

c) identifies the information security risks:

   1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and

   2) identify the risk owners;

d) analyses the information security risks:

   1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;

   2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and

   3) determine the levels of risk;

e) evaluates the information security risks:

   1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and

   2) prioritize the analysed risks for risk treatment.

The organization shall retain documented information about the information security risk assessment process.

6.1.3 Information security risk treatment

The organization shall define and apply an information security risk treatment process to:

a) select appropriate information security risk treatment options, taking account of the risk assessment results;

b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;

NOTE Organizations can design controls as required, or identify them from any source.

c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;

NOTE 1 Annex A contains a comprehensive list of control objectives and controls. Users of this Standard are directed to Annex A to ensure that no necessary controls are overlooked.

NOTE 2 Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed.

d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;

e) formulate an information security risk treatment plan; and

f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.

The organization shall retain documented information about the information security risk treatment process.

NOTE The information security risk assessment and treatment process in this Standard aligns with the principles and generic guidelines provided in ISO 31000[5].

6.2 Information security objectives and planning to achieve them

The organization shall establish information security objectives at relevant functions and levels.

The information security objectives shall:

a) be consistent with the information security policy;

b) be measurable (if practicable);

c) take into account applicable information security requirements, and results from risk assessment and risk treatment;

d) be communicated; and

e) be updated as appropriate.

The organization shall retain documented information on the information security objectives.

When planning how to achieve its information security objectives, the organization shall determine:

f) what will be done;

g) what resources will be required;

h) who will be responsible;

i) when it will be completed; and

j) how the results will be evaluated.

7 Support

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation.

7.2 Competence

The organization shall:

a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;

b) ensure that these persons are competent on the basis of appropriate education, training, or experience;

c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and

d) retain appropriate documented information as evidence of competence.

NOTE Applicable actions may include, for example: the provision of training to, the mentoring of, or the reassignment of current employees; or the hiring or contracting of competent persons.

7.3 Awareness

Persons doing work under the organization's control shall be aware of:

a) the information security policy;

b) their contribution to the effectiveness of the information security management system, including

c) the benefits of improved information security performance; and

d) the implications of not conforming with the information security management system requirements

7.4 Communication

The organization shall determine the need for internal and external communications relevant to the information security management system including:

a) on what to communicate;

b) when to communicate;

c) with whom to communicate;

d) who shall communicate; and

e) the processes by which communication shall be effected.

7.5 Documented information

7.5.1 General

The organization's information security management system shall include:

a) documented information required by this Standard; and

b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.

NOTE The extent of documented information for an information security management system can differ from one organization to another due to:

1) the size of organization and its type of activities, processes, products and services;

2) the complexity of processes and their interactions; and

3) the competence of persons.

7.5.2 Creating and updating

When creating and updating documented information the organization shall ensure appropriate:

a) identification and description (e.g. a title, date, author, or reference number);

b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and

c) review and approval for suitability and adequacy.

7.5.3 Control of documented information

Documented information required by the information security management system and by this Standard shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed; and

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:

c) distribution, access, retrieval and use;

d) storage and preservation, including the preservation of legibility;

e) control of changes (e.g. version control); and

f) retention and disposition.

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

NOTE Access implies a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

8 Operation

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.

The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that outsourced processes are determined and controlled.

8.2 Information security risk assessment

The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a).

The organization shall retain documented information of the results of the information security risk assessments.

8.3 Information security risk treatment

The organization shall implement the information security risk treatment plan.

The organization shall retain documented information of the results of the information security risk treatment.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organization shall evaluate the information security performance and the effectiveness of the information security management system.

The organization shall determine:

a) what needs to be monitored and measured, including information security processes and controls;

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

NOTE The methods selected should produce comparable and reproducible results to be considered valid.

c) when the monitoring and measuring shall be performed;

d) who shall monitor and measure;

e) when the results from monitoring and measurement shall be analysed and evaluated; and

f) who shall analyse and evaluate these results.

The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.

9.2 Internal audit

The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:

a) conforms to

1) the organization's own requirements for its information security management system; and

2) the requirements of this Standard;

b) is effectively implemented and maintained.

The organization shall:

c) plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;

d) define the audit criteria and scope for each audit;

e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

f) ensure that the results of the audits are reported to relevant management; and

g) retain documented information as evidence of the audit programme(s) and the audit results.

9.3 Management review

Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the information security management system;

c) feedback on the information security performance, including trends in:

    1) nonconformities and corrective actions;

    2) monitoring and measurement results;

    3) audit results; and

    4) fulfilment of information security objectives;

d) feedback from interested parties;

e) results of risk assessment and status of risk treatment plan; and

f) opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

The organization shall retain documented information as evidence of the results of management reviews.

10 Improvement

10.1 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:

    1) take action to control and correct it; and

    2) deal with the consequences;

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:

   1) reviewing the nonconformity;
   2) determining the causes of the nonconformity; and
   3) determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken; and

e) make changes to the information security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

The organization shall retain documented information as evidence of:

f) the nature of the nonconformities and any subsequent actions taken, and

g) the results of any corrective action.

10.2 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.

Annex A
(normative)
Reference control objectives and controls

The control objectives and controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2013[1], Clauses 5 to 18 and are to be used in context with Clause 6.1.3.

Table A.1 — Control objectives and controls

A.5 Information security policies		
A.5.1 Management direction for information security		
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.		
A.5.1.1	Policies for information security	*Control* A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.
A.5.1.2	Review of the policies for information security	Control The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
A.6 Organization of information security		
A.6.1 Internal organization		
Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.		
A.6.1.1	Information security roles and responsibilities	*Control* All information security responsibilities shall be defined and allocated.
A.6.1.2	Segregation of duties	*Control* Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
A.6.1.3	Contact with authorities	*Control* Appropriate contacts with relevant authorities shall be maintained.
A.6.1.4	Contact with special interest groups	*Control* Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.
A.6.1.5	Information security in project management	*Control* Information security shall be addressed in project management, regardless of the type of the project.

Table A.1 - (continued)

A.6.2 Mobile devices and teleworking		
Objective: To ensure the security of teleworking and use of mobile devices.		
A.6.2.1	Mobile device policy	*Control* A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.
A.6.2.2	Teleworking	*Control* A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.
A.7 Human resource security		
A.7.1 Prior to employment		
Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.		
A.7.1.1	Screening	*Control* Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
A.7.1.2	Terms and conditions of employment	*Control* The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.
A.7.2 During employment		
Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.		
A.7.2.1	Management responsibilities	*Control* Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.
A.7.2.2	Information security awareness, education and training	*Control* All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.
A.7.2.3	Disciplinary process	*Control* There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

Table A.1 - (continued)

A.7.3 Termination and change of employment		
Objective: To protect the organization's interests as part of the process of changing or terminating employment.		
A.7.3.1	Termination or change of employment responsibilities	*Control* Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.
A.8 Asset management		
A.8.1 Responsibility for assets		
Objective: To identify organizational assets and define appropriate protection responsibilities.		
A.8.1.1	Inventory of assets	*Control* Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.
A.8.1.2	Ownership of assets	*Control* Assets maintained in the inventory shall be owned.
A.8.1.3	Acceptable use of assets	*Control* Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.
A.8.1.4	Return of assets	*Control* All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.
A.8.2 Information classification		
Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.		
A.8.2.1	Classification of information	*Control* Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.
A.8.2.2	Labelling of information	*Control* An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
A.8.2.3	Handling of assets	*Control* Procedures for handling assets shall be developed and implementedin accordance with the information classification scheme adopted by the organization.

Table A.1 - (continued)

A.8.3 Media handling		
Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.		
A.8.3.1	Management of removable media	*Control* Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.
A.8.3.2	Disposal of media	*Control* Media shall be disposed of securely when no longer required, using formal procedures.
A.8.3.3	Physical media transfer	*Control* Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.
A.9 Access control		
A.9.1 Business requirements of access control		
Objective: To limit access to information and information processing facilities.		
A.9.1.1	Access control policy	*Control* An access control policy shall be established, documented and reviewed based on business and information security requirements.
A.9.1.2	Access to networks and network services	*Control* Users shall only be provided with access to the network and network services that they have been specifically authorized to use.
A.9.2 User access management		
Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.		
A.9.2.1	User registration and deregistration	*Control* A formal user registration and de-registration process shall be implemented to enable assignment of access rights.
A.9.2.2	User access provisioning	*Control* A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.
A.9.2.2	User access provisioning	*Control* A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.

Table A.1 - (continued)

A.9.2.3	Management of privileged access rights	*Control* The allocation and use of privileged access rights shall be restricted and controlled.
A.9.2.4	Management of secret authentication information of users	*Control* The allocation of secret authentication information shall be controlled through a formal management process.
A.9.2.5	Review of user access rights	*Control* Asset owners shall review users' access rights at regular intervals.
A.9.2.6	Removal or adjustment of access rights	*Control* The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
A.9.3 User responsibilities		
Objective: To make users accountable for safeguarding their authentication information.		
A.9.3.1	Use of secret authentication information	*Control* Users shall be required to follow the organization's practices in the use of secret authentication information.
A.9.4 System and application access control		
Objective: To prevent unauthorized access to systems and applications.		
A.9.4.1	Information access restriction	*Control* Access to information and application system functions shall be restricted in accordance with the access control policy.
A.9.4.2	Secure log-on procedures	*Control* Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.
A.9.4.3	Password management system	*Control* Password management systems shall be interactive and shall ensure quality passwords.
A.9.4.4	Use of privileged utility programs	*Control* The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
A.9.4.5	Access control to program source code	*Control* Access to program source code shall be restricted.

Table A.1 - (continued)

A.10 Cryptography		
A.10.1 Cryptographic controls		
Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.		
A.10.1.1	Policy on the use of cryptographic controls	*Control* A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
A.10.1.2	Key management	*Control* A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.
A.11 Physical and environmental security		
A.11.1 Secure areas		
Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.		
A.11.1.1	Physical security perimeter	*Control* Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.
A.11.1.2	Physical entry controls	*Control* Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
A.11.1.3	Securing offices, rooms and facilities	*Control* Physical security for offices, rooms and facilities shall be designed and applied.
A.11.1.4	Protecting against external and environmental threats	*Control* Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.
A.11.1.5	Working in secure areas	*Control* Procedures for working in secure areas shall be designed and applied.
A.11.1.6	Delivery and loading areas	*Control* Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

Table A.1 - (continued)

A.11.2 Equipment		
Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.		
A.11.2.1	Equipment siting and protection	*Control* Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
A.11.2.2	Supporting utilities	*Control* Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
A.11.2.3	Cabling security	*Control* Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.
A.11.2.4	Equipment maintenance	*Control* Equipment shall be correctly maintained to ensure its continued availability and integrity.
A.11.2.5	Removal of assets	*Control* Equipment, information or software shall not be taken off-site without prior authorization.
A.11.2.6	Security of equipment and assets off-premises	*Control* Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.
A.11.2.7	Secure disposal or reuse of equipment	*Control* All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
A.11.2.8	Unattended user equipment	*Control* Users shall ensure that unattended equipment has appropriate protection.
A.11.2.9	Clear desk and clear screen policy	*Control* A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

Table A.1 - (continued)

A.12 Operations security		
A.12.1 Operational procedures and responsibilities		
Objective: To ensure correct and secure operations of information processing facilities.		
A.12.1.1	Documented operating procedures	*Control* Operating procedures shall be documented and made available to all users who need them.
A.12.1.2	Change management	*Control* Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.
A.12.1.3	Capacity management	*Control* The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
A.12.1.4	Separation of development, testing and operational environments	*Control* Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.
A.12.2 Protection from malware		
Objective: To ensure that information and information processing facilities are protected against malware.		
A.12.2.1	Controls against malware	*Control* Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.
A.12.3 Backup		
Objective: To protect against loss of data.		
A.12.3.1	Information backup	*Control* Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.
A.12.4 Logging and monitoring		
Objective: To record events and generate evidence.		
A.12.4.1	Event logging	*Control* Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
A.12.4.2	Protection of log information	*Control* Logging facilities and log information shall be protected against tampering and unauthorized access.
A.12.4.3	Administrator and operator logs	*Control* System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

Table A.1 - (continued)

A.12.4.4	Clock synchronisation	*Control* The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.
A.12.5 Control of operational software		
Objective: To ensure the integrity of operational systems.		
A.12.5.1	Installation of software on operational systems	*Control* Procedures shall be implemented to control the installation of software on operational systems.
A.12.6 Technical vulnerability management		
Objective: To prevent exploitation of technical vulnerabilities.		
A.12.6.1	Management of technical vulnerabilities	*Control* Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
A.12.6.2	Restrictions on software installation	*Control* Rules governing the installation of software by users shall be established and implemented.
A.12.7 Information systems audit considerations		
Objective: To minimise the impact of audit activities on operational systems.		
A.12.7.1	Information systems audit controls	*Control* Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.
A.13 Communications security		
A.13.1 Network security management		
Objective: To ensure the protection of information in networks and its supporting information processing facilities.		
A.13.1.1	Network controls	*Control* Networks shall be managed and controlled to protect information in systems and applications.
A.13.1.2	Security of network services	*Control* Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.
A.13.1.3	Segregation in networks	*Control* Groups of information services, users and information systems shall be segregated on networks.

Table A.1 - (continued)

A.13.2 Information transfer		
Objective: To maintain the security of information transferred within an organization and with any external entity.		
A.13.2.1	Information transfer policies and procedures	*Control* Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.
A.13.2.2	Agreements on information transfer	*Control* Agreements shall address the secure transfer of business information between the organization and external parties.
A.13.2.3	Electronic messaging	*Control* Information involved in electronic messaging shall be appropriately protected.
A.13.2.4	Confidentiality or nondisclosure agreements	*Control* Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.
A.14 System acquisition, development and maintenance		
A.14.1 Security requirements of information systems		
Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.		
A.14.1.1	Information security requirements analysis and specification	*Control* The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.
A.14.1.2	Securing application services on public networks	*Control* Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.
A.14.1.3	Protecting application services transactions	*Control* Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

Table A.1 - (continued)

A.14.2 Security in development and support processes		
Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.		
A.14.2.1	Secure development policy	*Control* Rules for the development of software and systems shall be established and applied to developments within the organization.
A.14.2.2	System change control procedures	*Control* Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.
A.14.2.3	Technical review of applications after operating platform changes	*Control* When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
A.14.2.4	Restrictions on changes to software packages	*Control* *Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.*
A.14.2.5	Secure system engineering principles	*Control* *Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.*
A.14.2.6	Secure development environment	*Control* *Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.*
A.14.2.7	Outsourced development	*Control* *The organization shall supervise and monitor the activity of outsourced system development.*
A.14.2.8	System security testing	*Control* *Testing of security functionality shall be carried out during development.*
A.14.2.9	System acceptance testing	*Control* *Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.*
A.14.3 Test data		
Objective: To ensure the protection of data used for testing.		
A.14.3.1	Protection of test data	*Control* Test data shall be selected carefully, protected and controlled.

Table A.1 - (continued)

A.15 Supplier relationships		
A.15.1 Information security in supplier relationships		
Objective: To ensure protection of the organization's assets that is accessible by suppliers.		
A.15.1.1	Information security policy for supplier relationships	*Control* Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.
A.15.1.2	Addressing security within supplier agreements	*Control* *All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.*
A.15.1.3	Information and communication technology supply chain	*Control* *Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.*
A.15.2 Supplier service delivery management		
Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.		
A.15.2.1	Monitoring and review of supplier services	*Control* Organizations shall regularly monitor, review and audit supplier service delivery.
A.15.2.2	Managing changes to supplier services	*Control* Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.
A.16 Information security incident management		
A.16.1 Management of information security incidents and improvements		
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.		
A.16.1.1	Responsibilities and procedures	*Control* Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.
A.16.1.2	Reporting information security events	*Control* Information security events shall be reported through appropriate management channels as quickly as possible.

Table A.1 - (continued)

A.16.1.3	Reporting information security weaknesses	*Control* Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.
A.16.1.4	Assessment of and decision on information security events	*Control* Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.
A.16.1.5	Response to information security incidents	*Control* Information security incidents shall be responded to in accordance with the documented procedures.
A.16.1.6	Learning from information security incidents	*Control* Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
A.16.1.7	Collection of evidence	*Control* The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.
A.17 Information security aspects of business continuity management		
A.17.1 Information security continuity		
Objective: Information security continuity shall be embedded in the organization's business continuity management systems.		
A.17.1.1	Planning information security continuity	*Control* The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.
A.17.1.2	Implementing information security continuity	*Control* The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.
A.17.1.3	Verify, review and evaluate information security continuity	*Control* *The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.*
A.17.2 Redundancies		
Objective: To ensure availability of information processing facilities.		
A.17.2.1	Availability of information processing facilities	*Control* Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

Table A.1 - (continued)

A.18 Compliance		
A.18.1 Compliance with legal and contractual requirements		
Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.		
A.18.1.1	Identification of applicable legislation and contractual requirements	*Control* All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.
A.18.1.2	Intellectual property rights	*Control* Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.
A.18.1.3	Protection of records	*Control* Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance withlegislatory, regulatory, contractual and business requirements.
A.18.1.4	Privacy and protection of personally identifiable information	*Control* Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.
A.18.1.5	Regulation of cryptographic controls	*Control* *Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.*
A.18.2 Information security reviews		
Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.		
A.18.2.1	Independent review of information security	*Control* The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.
A.18.2.2	Compliance with security policies and standards	*Control* Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.
A.18.2.3	Technical compliance review	*Control* Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.

Bibliography

[1] ISO/IEC 27002:2013, *Information technology — Security Techniques — Code of practice for information security controls*

[2] ISO/IEC 27003, *Information technology — Security techniques — Information security management system implementation guidance*

[3] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Measurement*

[4] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[5] ISO 31000:2009, *Risk management — Principles and guidelines*

[6] ISO/IEC Directives, Part 1, *Consolidated ISO Supplement – Procedures specific to ISO*, 2012